UNITED STATES DISTRICT COURT
FOR DISTRICT OF MINNESOTA

Kayla Harris and Stephanie Braulick, individually, and on behalf of those similarly situated, Plaintiffs, v. Gillette Children's Specialty Healthcare, a Minnesota nonprofit corporation, Defendant.	Case No. **COMPLAINT - CLASS ACTION** **JURY TRIAL DEMANDED**

Plaintiffs Kayla Harris and Stephanie Braulick ("Plaintiffs"), individually and on behalf of themselves and all others similarly situated, by and through their attorneys of record, assert the following against Defendant Gillette Children's Specialty Healthcare ("Gillette" or "Defendant").

INTRODUCTION

1. This class action arises out of Gillette's unlawful use of third-party tracking technologies (the "Tracking Tools") to surreptitiously intercept and disclose its patients' private and protected communications, including communications concerning highly sensitive personal health information, to third parties, without patients' knowledge or consent. By purposely embedding and deploying the Tracking Tools on Gillette's website, www.gillettechildrens.org, Gillette engages in the unauthorized disclosure of its patients' highly sensitive Personal Health Information ("PHI") and Personally Identifiable Information ("PII") (collectively "Personal Information") to third parties, including, but

not limited to, Meta Platforms, Inc. d/b/a/ Meta ("Facebook") and Google LLC ("Google").[1] Such disclosures of Personal Information violate state and federal law.

2. Gillette is a nonprofit corporation headquartered in Minnesota that provides primary care and research services related to children's health issues. Gillette serves approximately 25,000 patients annually and generates approximately $300 million in annual revenue. In its ordinary course of business, Gillette encourages patients and prospective patients to use www.gillettechildrens.org (the "Website") to communicate about symptoms and conditions, research treatments, lookup physicians, and schedule appointments. Unbeknownst to its patients and prospective patients, these communications are intercepted and disclosed to third parties through Gillette's use of the Tracking Tools.

3. One of the Tracking Tools Gillette deployed on its website is the Meta Pixel ("Pixel").[2] Pixel is a snippet of code that, when embedded on a website, tracks the website visitor's activity on that website and sends that data to a third party, like Meta. This includes tracking and logging pages and subpages the website user visits during a website session that reveal patient status and other personal identifying and protected health information, searches, and other submissions to the website, which in many cases includes sensitive personal and identifying information that is not anonymized. Indeed, Pixel is routinely used

[1] While this complaint focuses on tracking tools from Facebook and Google, research shows that Defendant also embedded tracking codes from a number of other marketing companies including Bing, Colossus SSP, LinkedIn, Microsoft Clarity, PubMatic, Inc., ScorecardResearch, SiteScout, StickyADS.tv, Teads, The Trade Desk, and Yahoo.

[2] Meta also provides other tracking technologies that give the same or similar tracking functionalities as Pixel, including, but not limited to, Conversions API, SDKs, and Audiences. Absent discovery, Plaintiffs are unable to independently confirm whether Defendant installed such tracking technologies on the Website.

to target specific individuals by utilizing the data gathered through Pixel to build profiles for the purpose of future targeting and marketing. Here, the information transmitted to third-party Meta without Plaintiffs' consent included private health information,[3] which is some of the most personal and sensitive data Plaintiffs have.

4. Additionally, when a patient communicates with Gillette's Website where Pixel is present, Pixel source code causes the exact content of the patients' communications with the Website to be re-directed to Meta in a way that identifies the person as a patient. Here, for example, Plaintiffs used the Website to communicate about their children's sensitive health conditions and symptoms and to research potential treatments and physicians.[4] Unbeknownst to Plaintiffs, when they communicated about their children's personal health information, Pixel secretly intercepted, recorded, and transmitted those private communications to Meta along with unique identifiers Meta could use to identify Plaintiffs. Specifically, Defendant used Pixel to intercept its users' sensitive communications and have those communications associated with Facebook user profiles for purposes of future ad targeting and marketing.

---

[3] Under HIPAA, "health information" is defined as "any information[], whether oral or recorded in any form or medium, that . . . [i]s created or received by a health care provider . . . and [r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual." 45 C.F.R. § 160.103. Additionally, HIPAA defines "health care" as "care, services, or supplies related to the health of an individual" and includes, but is not limited to, the "[s]ale or dispensing of drug, device, equipment, or other item in accordance with a prescription." *Id.*

[4] Under HIPAA, the Plaintiff parents are treated as the "patient" of Gillette with respect to any disclosures of their children's personal health information. *See* 45 C.F.R. § 164.502(g)(1), (g)(3).

5. As a result of Defendant's use of Pixel, Plaintiffs' and Class Members' Personal Information, including, but not limited to, computer IP addresses; patient status; health conditions and symptoms; treatments; physicians; appointment details; and unique personal identifiers used to link the sensitive web communications to Plaintiffs and the Class, was compromised and disclosed to third parties such as Meta without authorization or consent.

6. Such private information would allow Meta to know that a specific patient was seeking confidential health care or exploring treatment for a specific condition.

7. Defendant's Tracking Tools have also transmitted patients' Personal Information to additional unauthorized third parties for marketing and advertising purposes, including Google.

8. Google's tracking technologies operate much like the Meta Pixel. As one District Court recently described:

> Whenever a user visits a website that is running Google Analytics, Ad Manager, or some similar Google service, Google's software directs the user's browser to send a separate communication to Google. This happens even when users are in private browsing mode, unbeknownst to website developers or the users themselves. The operation is not in dispute. When a user visits a website, the user's browser sends a "GET" request to the website to retrieve it. This GET request contains the following information: the Request URL, or the URL of the specific webpage the user is trying to access; the user's IP address; the User-agent, which identifies the user's device platform and browser; user's geolocation, if available; the Referer, which is the URL of the page on which the user clicked a link to access a new page; event data, which describes how users interact with a website, for example, whether they saw an ad or played a video; and the actual search queries on the site. At the same time, the user's browser reads Google's code, which is embedded on the website. Google's code instructs the user's browser to send a second and concurrent transmission

directly to Google. This second transmission tells Google exactly what a user's browser communicated to the website.[5]

9. In secretly deploying the Tracking Tools on its Website to intercept and disclose website communications concerning its patients' and prospective patients' Personal Information, Defendant acted with a tortious and criminal purpose in violation of state and federal laws.

10. Plaintiffs and the Class Members never consented to, authorized, or otherwise agreed to allow Defendant to disclose their Personal Information to anyone other than those reasonably believed to be part of Gillette, acting in some healthcare-related capacity. Despite this, Defendant knowingly and intentionally disclosed Plaintiffs' and the Class Members' Personal Information to Meta, Google, and other potential third parties.

11. Given the nature of Meta and Google's businesses as two of the world's largest online advertising companies, Plaintiffs' and the Class Members' Personal Information can and will likely be further used by or exposed to additional third parties.

12. As a direct and proximate result of Defendant's unauthorized exposure of Plaintiffs' and the Class Members' Personal Information, Plaintiffs and the Class Members have suffered injury, including an invasion of privacy; loss of the benefit of the bargain Plaintiffs and the Class Members considered at the time they bargained for healthcare

[5] *Brown v. Google LLC*, No. 4:20-CV-3664-YGR, 2023 WL 5029899, at *2 (N.D. Cal. Aug. 7, 2023). As explained by the Court in *Brown*, Google connects user data to IP addresses; IP addresses have been classified by the United States Department of Health and Human Services ("HHS") as personally identifiable information that constitutes one of the 18 HIPAA identifiers of PHI. *See* 45 C.F.R. § 164.514 (2).

services and agreed to use Defendant's Website for services; statutory damages; and the continued and ongoing risk to their Personal Information.

13. Accordingly, Plaintiffs bring this action individually, and on behalf of a Class of similarly situated individuals, to recover for harms suffered and assert the following claims: Violations of the Electronic Communications Privacy Act ("ECPA") (18 U.S.C. § 2511); Invasion of Privacy; Negligence; Breach of Implied Contract; Unjust Enrichment; and the Minnesota Uniform Deceptive Trade Practices Act ("MUDTPA"), Mn. Stat. §325D.43-48.

PARTIES

14. **Plaintiff Kayla Harris** is a natural person who resides and intends to remain in Minnesota. At all relevant times, Harris was a citizen of Minnesota.

15. **Plaintiff Stephanie Braulick** is a natural person who resides and intends to remain in Minnesota. At all relevant times, Braulick was a citizen of Minnesota.

16. **Defendant Gillette Specialty Healthcare** is a Minnesota nonprofit corporation headquartered at 200 E University Ave., St Paul, MN 55101.

JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction under 28 U.S.C. § 1331 because this Complaint asserts claims pursuant to Defendant's violations of the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2511.

18. This court has supplemental jurisdiction over Plaintiffs' state law claims under 28 U.S.C. § 1367.

19. This Court has personal jurisdiction over Defendant because Gillette is a Minnesota nonprofit corporation with its principal place of business in this District.

20. Venue is proper under 28 U.S.C. §§ 1391(b)(1) – (2) because Defendant's principal place of business is in this District and because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District.

FACTUAL ALLEGATIONS

A. Federal Regulators Have Warned Healthcare Providers About the Impermissible Use of Tracking Technologies

21. The surreptitious collection and disclosure of Personal Information is an extremely serious data security and privacy issue. Both the Federal Trade Commission ("FTC") and the Office for Civil Rights of the U.S. Department of Health and Human Services ("HHS") have recently reiterated the necessity for data security and privacy concerning health information.

22. For instance, the FTC recently published a bulletin entitled *Protecting the privacy of health information: A baker's dozen takeaways from FTC cases*, in which it noted that "[h]ealth information is not just about medications, procedures, and diagnoses. Rather, it is anything that conveys information—or enables an inference—about a consumer's health. Indeed, [recent FTC enforcement actions involving] Premom, BetterHelp, GoodRx and Flo Health make clear that the fact that a consumer is using a particular health-related app or website—one related to mental health

or fertility, for example—or how they interact with that app (say, turning 'pregnancy mode' on or off) may itself be health information."[6]

23. The FTC is unequivocal in its stance as it informs—in no uncertain terms—companies that provide healthcare services that they should not use tracking technologies to collect sensitive health information and disclose it to various platforms without informed consent:

> **Don't use behind-the-scenes tracking technologies that contradict your privacy promises or otherwise harm consumers.** In today's surveillance economy, the consumer is often the product. Consumer data powers the advertising machine that goes right back to the consumer. But when companies use consumers' sensitive health data for marketing and advertising purposes, such as by sending that data to marketing firms via tracking pixels on websites or software development kits on apps, watch out. [Recent FTC enforcement actions such as] *BetterHelp*, *GoodRx*, *Premom*, and *Flo* make clear that practices like that may run afoul of the FTC Act if they violate privacy promises or if the company fails to get consumers' affirmative express consent for the disclosure of sensitive health information.[7]

24. In December 2022, HHS similarly warned healthcare providers that, "Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules."[8] The HHS Privacy Bulletin also made clear that,

---

[6] *See* Elisa Jillison, *Protecting the privacy of health information: A Baker's dozen takeaways from FTC cases,* the FTC Business Blog (July 25, 2023), https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases (last visited Apr. 18, 2024).

[7] *Id.* (emphasis added).

[8] *See Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-

"disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures."[9]

25. In July 2023, the FTC and HHS sent a letter to approximately 130 healthcare providers warning them about the use of online tracking technologies that could result in unauthorized disclosures of Personal Information to third parties.[10] The letter highlighted the "risks and concerns about the use of technologies, such as the Meta/Facebook pixel and Google Analytics, that can track a user's online activities," and warned about "[i]mpermissible disclosures of an individual's personal health information to third parties" that could "result in a wide range of harms to an individual or others."[11] According to the letter, "[s]uch disclosures can reveal sensitive information including health conditions, diagnoses, medications, medical treatments, frequency of visits to health care professionals, where an individual seeks medical treatment, and more."[12]

26. In March 2024, HHS reiterated its warning to healthcare providers, stating that "[w]hile it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, because of the proliferation of tracking technologies collecting sensitive information, OCR is providing this reminder that it is critical for

---

tracking/index.html ("HHS Privacy Bulletin"). The original guidance was issued in December 2022 and was recently updated in March 2024.

[9] *Id.*

[10] https://www.ftc.gov/business-guidance/blog/2023/07/ftc-hhs-joint-letter-gets-heart-risks-tracking-technologies-pose-personal-health-information

[11] https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf

[12] *Id.*

regulated entities to ensure that they disclose PHI **only** as expressly permitted or required by the HIPAA Privacy Rule."[13]

27. Despite these clear warnings from federal regulators, Defendant Gillette embedded Tracking Tools on its Website to secretly track its patients' communications regarding healthcare information and disclose those communications to third parties.

B. The Meta Pixel

28. Through its Website, Defendant connects Plaintiffs and the Class Members to Defendant's digital health care platform with a core goal of increasing profitability.

29. In furtherance of that goal, and to increase the success of its advertising and marketing, Defendant purposely embedded and deployed Meta Pixel on its Website. By doing so, Defendant surreptitiously shared its patients' and prospective patients' identities and online activity, including private communications and search results related to conditions, symptoms, treatments, and physicians, with Meta.

30. Meta's core business function is to sell advertising, and it does so on several platforms, including Facebook and Instagram. The bulk of Meta's billions of dollars in annual revenue comes from advertising—a practice in which Meta actively participates by using algorithms that approve and deny ads based on the ads' content, human moderators that further review ads for both legality and aesthetics prior to and after the ads are published, and other algorithms that connect ads to specific users, without the assistance or input of the advertiser.

[13] *See supra*, note 8 (emphasis in original).

31. Over the last decade, Facebook, now Meta, has become one of the largest and fastest growing online advertisers in the world. Since its creation in 2004, Facebook's daily, monthly, and annual user base has grown exponentially to billions of users.

32. Meta's advertising business has been successful due, in significant part, to Meta's ability to target users, both based on information users provide to Meta, and based on other information about users Meta extracts from the Internet at large. Given the highly specific data used to target particular users, thousands of companies and individuals utilize Facebook's advertising services.

33. One of Meta's most powerful advertising tools is the Meta Pixel (formerly the "Facebook Pixel"), which it first launched in 2015.

34. Meta branded Pixel as "a new way to report and optimize for conversions, build audiences and get rich insights about how people use your website." Meta further stated:

> Facebook pixel, [is] a new way to report and optimize for conversions, build audiences[,] and get rich insights about how people use your website. We're also announcing the availability of custom conversions, a new rule-based method to track and report conversions for your Facebook ads.
>
> Facebook pixel makes things simple for advertisers by combining the functionality of the Conversion Tracking pixels and Custom Audience pixels into a single pixel. You only need to place a single pixel across your entire website to report and optimize for conversions. Since it is built on top of the upgraded Custom Audience pixel, all the features announced in our previous blog post (Announcing Upgrades to Conversion Tracking and Optimization at Facebook) are supported through Facebook pixel as well.
> [Advertisers and website operators] can use Facebook pixel to track and optimize for conversions by adding standard events (*e.g.*, Purchase) to your

Facebook pixel base code on appropriate pages (*e.g.*, purchase confirmation page).[14]

35. Pixel is an easily attainable piece of code that Meta makes available to website developers for free. In exchange, at a minimum, website developers must agree to Meta's Business Tool Terms.[15]

36. The Business Tool Terms note that the Meta's Business Tools, including Pixel, will capture two types of information: "Contact Information" which "personally identifies individuals," and "Event Data" which contains additional information about people and their use of a developer's website.[16]

37. The Business Tools Terms also require websites to "provide[] robust and sufficiently prominent notice to users . . . on each web page where our pixels are used that links to a clear explanation (a) that third parties, including Meta, may . . . collect or receive information from your websites and elsewhere on the Internet and use that information to . . . deliver ads, (b) how users can opt out of the collection and use of information . . . and (c) where a user can access a mechanism for exercising such choice[.]"[17]

---

[14] Cecile Ho, *Announcing Facebook Pixel*, Meta (Oct. 14, 2015), https://developers.facebook.com/ads/blog/post/v2/2015/10/14/announcing-facebook-pixel/ (last visited Apr. 14, 2024).

[15] *See* Meta Business Tool Terms, https://www.facebook.com/legal/businesstech?paipv=0&eav=AfaHqYwiwGYZ0X0vZZ1I5uQ1zuI0STn-VURAyVhvlzw1Df5nxIgiuXOqcd5A8yKuEtk&_rdr ("When you use any of the Meta Business Tools . . . or otherwise enable the collection of Business Tool Data . . . these Business Tool Terms govern the use of that data") (last visited Apr. 22, 2024).

[16] *Id.* at Section 1(a)(i)-(ii)

[17] *Id.* at Section 3(c)(i)

38. However, even with all of these protocols in place, Meta flatly prohibits the disclosure of Business Tools Data "that you know or reasonably should know . . . includes health, financial information or other categories of sensitive information (including any information defined as sensitive under applicable laws, regulations and applicable industry guidelines)."[18]

39. After agreeing to the Business Tools Terms, website developers can choose to install and use Pixel on their websites to track and measure certain actions, such as a website visitor's text searches and page views, including the detailed URLs triggered by page views. When a website visitor takes an action a developer chooses to track on its website, Pixel is triggered and sends data about that "Event" to Meta. All of this happens without the user's knowledge or consent.

40. Web browsers are software applications that allow consumers to navigate the web and view and exchange electronic information and communications over the Internet. Each "client device" (such as a computer, tablet, or smart phone) accesses web content through a web browser (*e.g.*, Google's Chrome browser, Mozilla's Firefox browser, Apple's Safari browser, and Microsoft's Edge browser).

41. Every website is hosted by a computer "server" that holds the website's contents and through which the entity in charge of the website exchanges communications with Internet users' client devices via their web browsers.

[18] *Id.* at Section 1(h).

42. Ultimately, a browsing session online may consist of thousands of web communications. Web communications consist of HTTP or HTTPS Requests and HTTP or HTTPS Responses, and any given browsing session may consist of thousands of individual HTTP Requests and HTTP Responses, along with corresponding cookies:

- An **HTTP Request** is an electronic communication a website visitor sends from his device's browser to the website's server. There are two types of HTTP Requests: (1) GET Requests, which are one of the most common types of HTTP Requests—in addition to specifying a particular URL (*i.e.*, web address), GET Requests can also send data to the host server embedded inside the URL, and can include cookies; and (2) POST Requests which can send a large amount of data outside of the URL. In this case, a patient's HTTP Request would be asking Defendant's Website to get certain information, such as a list of clinic locations or prescriptions. So that servers can better understand what information users are requesting, HTTP Requests also use URLs that contain parameters, which use variables and assigned values in the URL to pass additional information through the HTTP Request.

- **Cookies** are a text file that website operators and others use to store information on the website visitor's device; these can later be communicated to a server or servers. Cookies are sent with HTTP Requests from website visitor's devices to the host server. Some cookies are "third-party cookies," which means they can store and communicate data when visiting one website to an entirely different website. Third-party cookies are created by a website with a domain name other than the one the user is visiting, in this case Meta.[19] There are also "first-party cookies," like the fbp cookie, which is created by the website the user is visiting, in this case Defendant.[20] Meta uses both first- and third-party cookies in Pixel to link Facebook IDs and Facebook profiles, and Defendant sends these identifiers to Meta.

- An **HTTP Response** is a response to an HTTP Request. It is an electronic communication that is sent as a reply to the website visitor's device's web browser from the host server. HTTP responses may consist of a web page,

[19] *Third-Party Cookie*, https://www.pcmag.com/encyclopedia/term/third-party-cookie (last visited Apr. 21, 2024). This is also confirmable using web developer tools to inspect a website's cookies and track network activity.

[20] *First-Party Cookie*, https://www.pcmag.com/encyclopedia/term/first-party-cookie (last visited Apr. 21, 2024). This is also confirmable using web developer tools to inspect a website's cookies and track network activity.

> another kind of file, text information, or error codes, among other data. Basically, the HTTP Response is when the website sends the requested information (*see* the HTTP Request); this is sometimes called the "Markup."

43. A user's HTTP Request essentially asks the Defendant's Website to retrieve certain information (such as "Orthopedics"). The HTTP Response then renders or loads the requested information in the form of Markup (i.e., the pages, images, words, buttons, and other features that appear on the patient's screen as they navigate Defendant's Website).

44. Every website, including Defendant's, is composed of Markup and "Source Code." Source code is a set of instructions that commands the website visitor's browser to take certain actions when the web page loads or when a specified event triggers the code.

45. Source code may also command a web browser to transmit data to third parties in the form of an HTTP Request. Such data transmissions allow a website to export data about users and their actions to third parties. Third parties receiving this data are typically configured to track user data and communications for marketing purposes.

46. Transmission of a such data can be done quietly in the background without notifying the web browser's user. The pixels are invisible to website users and thus, without any knowledge, authorization, or action by the user, the website site developer (or website commander) can use its source code to contemporaneously and to invisibly re-direct the user's PII and other non-public medical information to third parties. Through Pixel, Defendant uses source code that can accomplish just that.

47. Pixel "tracks the people and the types of actions they take."[21] According to Meta, Pixel is a piece of code that allows Defendant to measure the effectiveness of [its] advertising by understanding the actions [website visitors] take on [its] website."[22] Thus, by secretly recording and transmitting data to Meta—without the user's knowledge or consent—Pixel acts much like a traditional wiretap controlled by Defendant.

48. Through this online tracking technology, Meta intercepts each page a user visits, what buttons they click, as well as the specific information the user inputs into the website and other searches conducted. Pixel sends each of these pieces of information to Meta with PII, such as the user's IP address. Meta stores this data on its own servers, in some instances for years on end, and independently uses the data for its own financial gain.

49. Importantly, this data is often associated with the individual user's Facebook account. For example, if the user is logged into their Facebook account (or has been logged in recently) when the user visits Defendant's website, Meta receives third-party cookies allowing Meta to link the data collected by Pixel to the specific Facebook user. In other words, a user's personal and private information sent by the Meta Pixel to Facebook is sent alongside that user's personal identifiers, including IP address and cookie values, which can be linked to the user's unique Facebook account.

50. Meta accomplishes this by placing cookies in the web browsers of users logged into their services, which aids Meta in identifying users.

---

[21] *Retargeting*, Facebook, https://www.facebook.com/business/goals/retargeting (last visited Apr. 21, 2024).

[22] *About Meta Pixel*, Meta Business Help Center, https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited Apr. 21, 2024).

51. One such example is the "c_user" cookie, which is a type of third-party cookie assigned to each person who has a Facebook account. The "c_user" cookie contains a numerical value known as the Facebook ID ("FID") that uniquely identifies a Facebook user. It is composed of a unique and persistent set of numbers. A user's FID is linked to their Facebook profile, which generally contains a wide range of demographic and other information about the user, including pictures, personal interests, work history, relationship status, and other details. Because the user's Facebook Profile ID uniquely identifies an individual's Facebook account, Meta—or any ordinary person—can easily use the Facebook Profile ID to quickly, and easily, locate, access, and view the user's corresponding Facebook profile. Thus, when a Facebook user visits Defendant's Website while logged in to their Facebook account, Pixel transmits the user's private web communications with the Defendant along with the "c_user" cookie. Meta can then use this information to match the web communications with the user's Facebook ID.

52. Even if a user does not have a Facebook account or is not logged in to Facebook when browsing the Defendant's Website, Pixel transmits the user's web communications with Defendant's Website to Meta along with a unique identifier associated with another cookie called the "_fbp" cookie. Meta can then use that unique identifier to link the user's web communications with the user's Facebook ID. And if a user who does not have a Facebook account later creates an account, Meta may be able to associate the user's historical browsing history intercepted via Pixel and "_fbp" cookie to the newly created account.

53. Meta's Business Tools Terms make clear that Pixel is meant to "match the Contact Information" of users "against user IDs . . . as well as to combine those user IDs with corresponding Event Data."[23]

54. After Meta is finished processing users' intercepted information, it makes the relevant analytics available to Gillette through Meta's Event Manager tool.

55. Using the Events Manager, Gillette can and is intended to review a summary of users' activity, including the pages, parameters and URLs sent through Pixel,[24] as well as any included metadata.[25]

56. Thus, without any knowledge, authorization, or action by a user, a website owner like Defendant can use its Source Code to commandeer the user's computing device, causing the device to contemporaneously and invisibly re-direct the users' communications to Meta. Meta then uses the information transmitted by Pixel to match the user with their Facebook ID.

---

[23] *Meta Business Tool Terms, Section 2(a)(i)(1)*, https://www.facebook.com/legal/businesstech?paipv=0&eav=AfaHqYwiwGYZ0X0vZZ1I5uQ1zuI0STn-VURAyVhvlzw1Df5nxIgiuXOqcd5A8yKuEtk&_rdr (last visited Apr. 22, 2024).

[24] *How to view pages, parameters and URLs in Meta Events Manager*, https://www.facebook.com/business/help/815029860145251 ("In Meta Events Manager, you can see a summary of pages, parameters and URLs recently sent through the Meta Pixel . . . .") (last visited Apr. 22, 2024).

[25] A web developer using the Events Manager can "[c]lick on the filter icon to select what activity types and details are display." Developers can sort by activity types, including "automatically logged pixel events," which may contain metadata. *Test your app or web browser events using the test events tool*, https://www.facebook.com/business/help/2040882565969969?id=1205376682832142 (last visited Apr. 22, 2024).

57. Judge William H. Orrick on the U.S. District Court for the Northern District of California summarized how this process plays out:

> To understand how the Meta Pixel typically works, imagine the following scenario. A shoe company wishes to gather certain information on customers and potential customers who visit its website. The shoe company first agrees to Meta's Business Tools Terms (discussed below), which govern the use of data from the Pixel. The shoe company then customizes the Meta Pixel to track, say, every time a site visitor clicks on the "sale" button on its website, which is called an "Event." Every time a user accesses the website and clicks on the "sale" button (i.e., an "Event" occurs), it triggers the Meta Pixel, which then sends certain data to Meta. Meta will attempt to match the customer data that it receives to Meta users—Meta cannot match non-Meta users. The shoe company may then choose to create "Custom Audiences" (i.e., all of the customers and potential customers who clicked on the "sale" button) who will receive targeted ads on Facebook, Instagram, and publishers within Meta's Audience Network. Meta may also provide the shoe company with de-identified, aggregated information so the shoe company understands the impact of its ads by measuring what happens when people see them. Meta does not reveal the identity of the matched Meta users to the shoe company.

In re Meta Pixel Healthcare Litig., No. 22-CV-03580-WHO, 2022 WL 17869218, at *2 (N.D. Cal. Dec. 22, 2022) (internal citations omitted).[26]

58. Pixel also allows a company, like Defendant, to impact the delivery of ads, measure cross-device conversions, create custom audiences, and save money on advertising and marketing costs.[27] But, most relevant here, Pixel allowed Defendant and

[26] In describing Pixel technology in *In re Meta Pixel Healthcare Litig.*, the court referenced the declaration of expert Richard M. Smith, which provides further details on the manner in which the challenged Pixel technology works and Meta's arrangements with health providers that employ it. 2022 WL 17869218, at *2. *See* Declaration of Richard M. Smith, filed in *In re Meta Pixel Healthcare Litig.*, No. 22-CV-03580-WHO (N.D. Cal.) [ECF 49].

[27] *Meta Pixel,* https://www.facebook.com/business/tools/meta-pixel?ref=search_new_2 (last visited Apr. 14, 2024).

Meta to track website users secretly on Defendant's Website and intercept their communications with Defendant.

59. When visitors to Defendant's Website, like Plaintiffs and the Class Members, communicated with Defendant or inquired about personal health-related topics, that information was transmitted to and intercepted by Meta.

60. The Personal Information intercepted, recorded, and transmitted to Meta includes, but is not limited to, patient status; health symptoms; health conditions; possible treatments; appointment details; bill payment details; and physicians. During that same transmission, Defendant would also provide Meta with the patient's Facebook ID number, other persistent cookies, device ID, computer IP addresses, or other PII. This information makes it easy to link private communications with Defendant via the Website to a specific and identifiable Facebook user.

61. Once Meta has that data, it processes it, analyzes it, and assimilates it into databases like Core Audiences or Custom Audiences for advertising purposes. If the website visitor is also a Facebook user, Meta will associate the information that it collects from the visitor with a Facebook ID that identifies the user's name and Facebook profile. In sum, Pixel allows Meta to learn, manipulate, and use for financial gain, the medical and private content Defendant's Website visitors communicated, viewed, or otherwise interacted with on Defendant's Website.

C. Google Tracking Code

62. Like the Meta Pixel, Google creates code that website developers can install on their websites to track user activity. Whenever a user visits a website that is running

Google tracking code, Google's code directs the user's browser to send a separate and concurrent communication to Google without the user's knowledge.

63. The information that is intercepted and transmitted to Google via the Google tracking code includes: the URL of the specific webpage the user is trying to access; the user's IP address; the User-agent, which identifies the user's device platform and browser; the user's geolocation, if available; the Referer, which is the URL of the page on which the user clicked a link to access a new page; event data, which describes how users interact with a website, for example, whether they saw an ad or played a video; and the actual search queries on the site. In this way, Google tracking code tells Google exactly what a user's browser communicated to the website.

64. Like with the Meta Pixel, the user's communications to the website are transmitted to Google together with cookies and other unique identifiers that Google can use to match the communications to individuals who use Google's services.

D. Gillette Deploys Third-Party Tracking Technologies To Intercept and Disclose Personal Information

65. As an example of how the Meta Pixel operated on Defendant's Website, consider a visitor who opens Defendant's Website, and navigates to the "Epilepsy and Seizures" webpage. When doing so, the visitor's browser sends a GET Request to Defendant's server, requesting that server to load the webpage displayed below in ***Figure 1***:

Figure 1: Depiction of Epilepsy Webpage

66. At the same time, Pixel causes the visitor's browser to secretly intercept and record the visitor's communication with Defendant's Website, including the specific URL requested, and transmit the private communication to Meta along with unique identifiers used to link the communication to a specific Facebook user, as shown in ***Figure 2***:

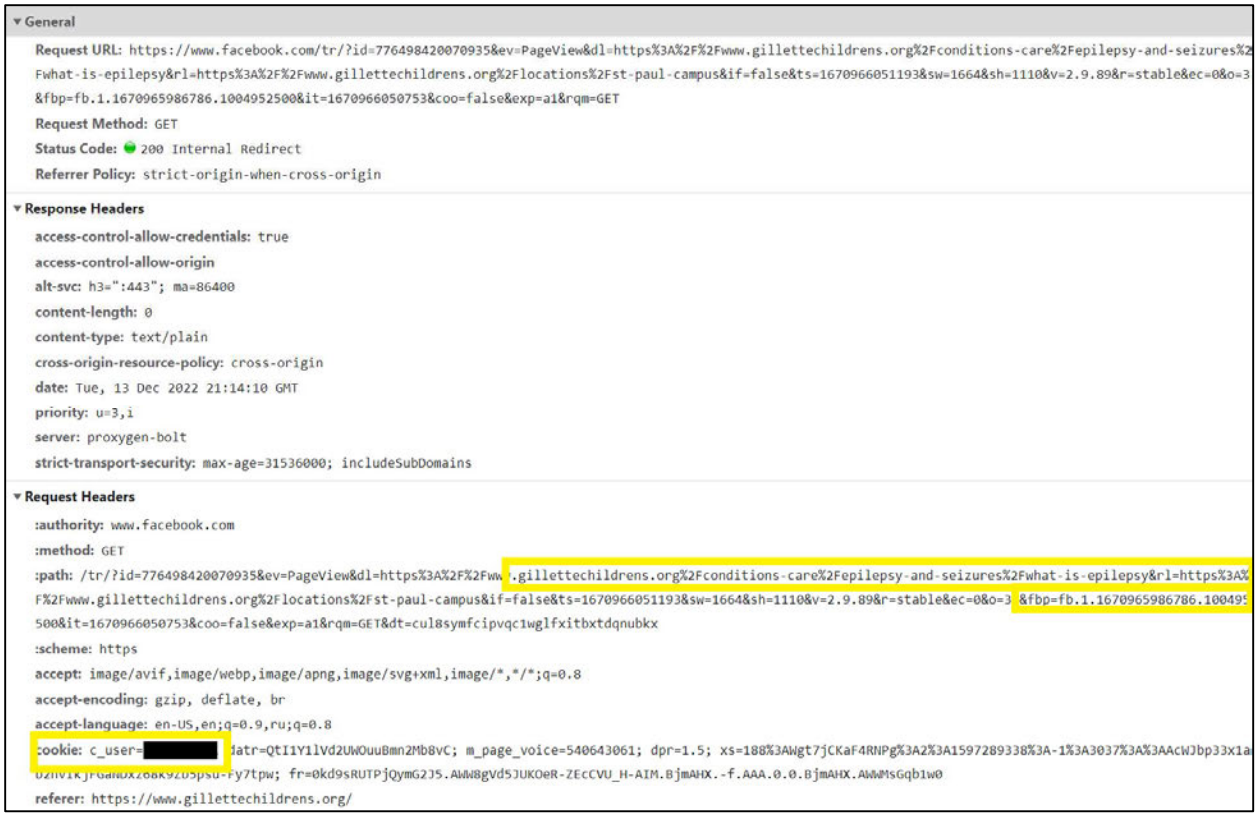

Figure 2: Depiction of information transmitted to Meta.

67. As reflected in ***Figure 2***, the "path" shows the specific URL for the page requested by the visitor's browser, including the substantive description "epilepsy and seizures." It also shows the Pixel's transmission of the _fbp cookie, the c_user cookie (the Facebook ID), and other cookies and identifiers used to identify the website visitor by name and Facebook account. Thus, the fact that a patient or prospective patient is using or considering using Gillette for healthcare services is transmitted to Meta. Disclosure of that information reveals to Meta the website visitor's status as a patient or prospective patient with Gillette.

68. If that same patient inquired about specific physicians through the Website's "Care Team" webpage, the Pixel would likewise intercept those communications and

transmit them to Meta along with the patient's unique identifiers, as reflected in ***Figure 3*** below:

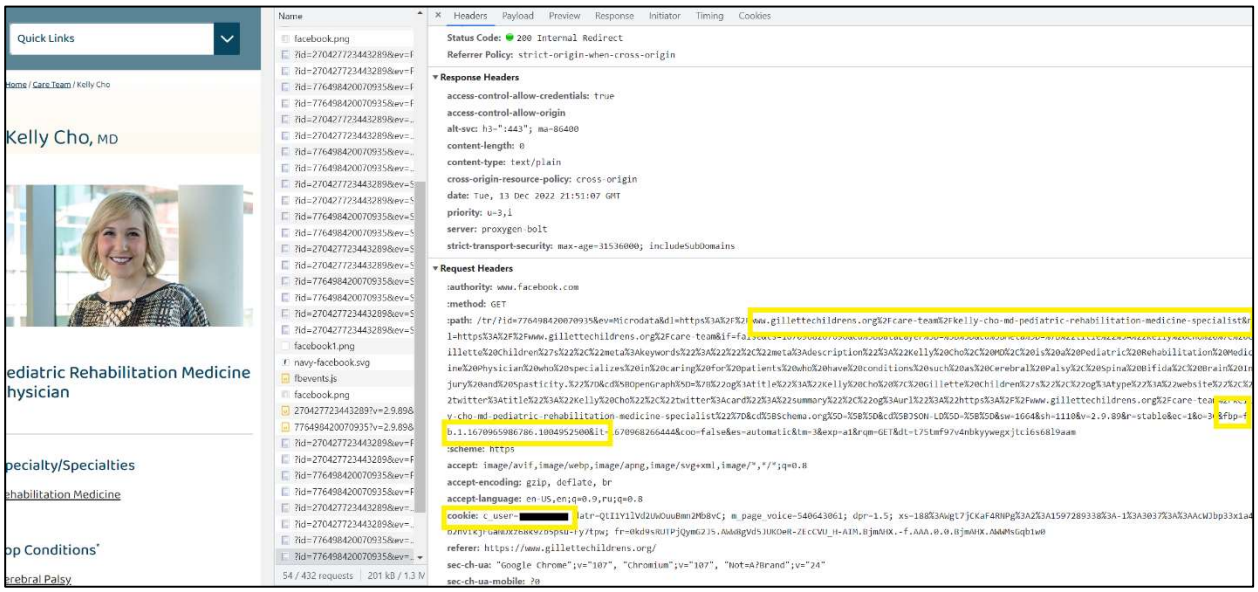

Figure 3: Depiction of search for physician

69. The Website provides an option for patients to click a button to call and make an appointment with a particular specialist. If the patient did click on the phone number to make an appointment, the Pixel would likewise intercept those communications, including the inner text of the button (here, the phone number for appointments with the provider) and transmit them to Meta along with the patient's unique identifiers, as reflected in ***Figures 4-5*** below:

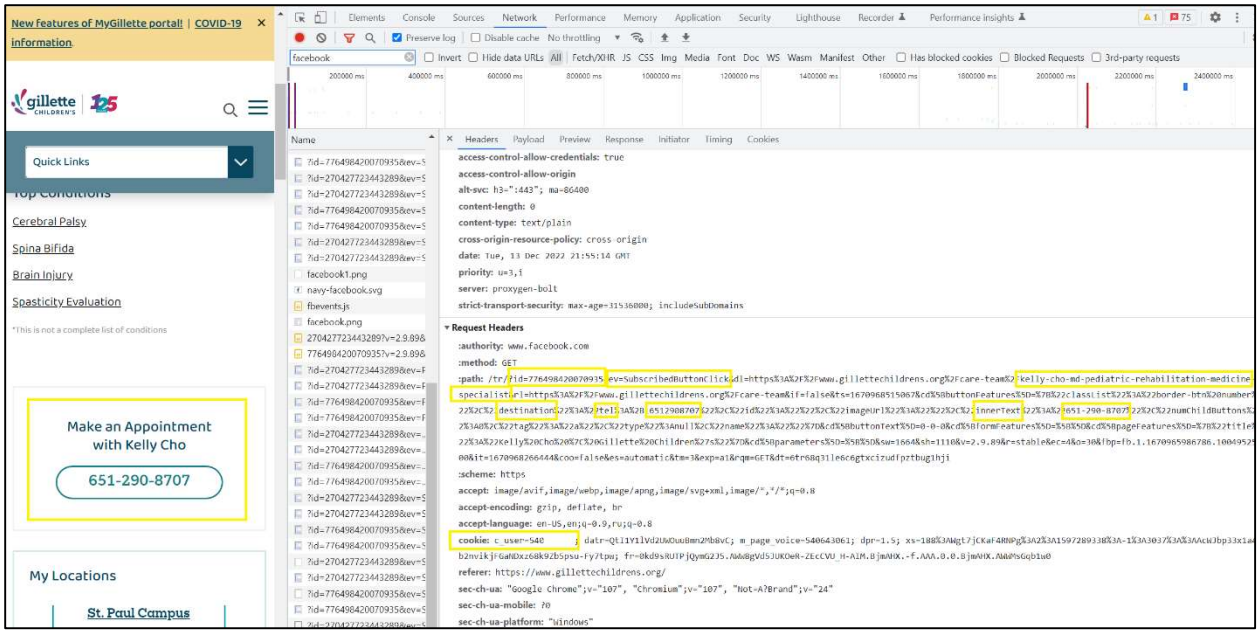

Figure 4: Depiction of a SubscribedButtonClick "event" disclosing that the patient is attempting to make an appointment with Dr. Cho, a pediatric rehabilitation medicine specialist.

Figure 5: A close-up of source code from Figure 4.

70. Gillette's deployment of the Google tracking code works in much the same way. If a patient inquired about brain injuries and symptoms, the patient's browser would send a GET request to Defendant's server to load the following webpage, as reflected in ***Figure 6***:

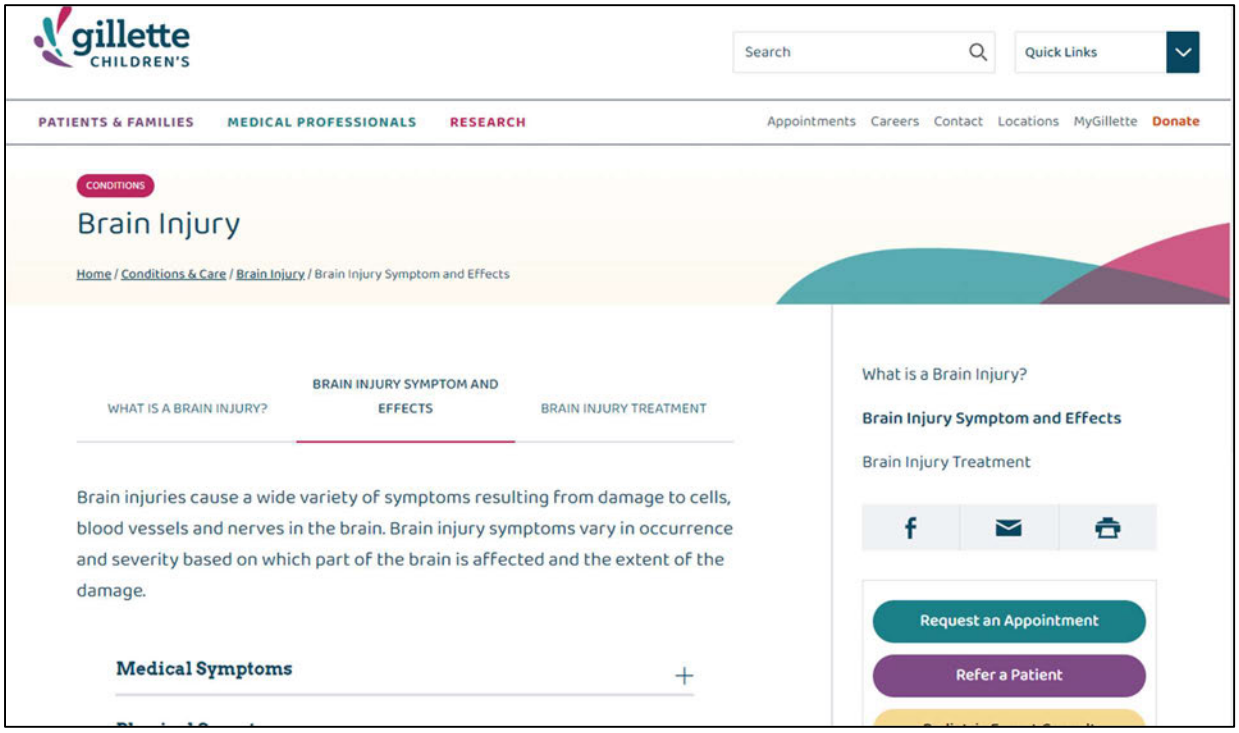

Figure 6: Depiction of Brain Injury Webpage

71. Because Defendant's Website deploys the Google tracking code, the patient's private communications to Defendant's Website are also intercepted and transmitted to Google along with unique identifiers used to link the communications to a specific Google user, including the "IDE" cookie used specifically for advertising,[28] as shown in ***Figure 7***:

[28] *Our advertising and measurement* cookies, https://business.safety.google/adscookies/

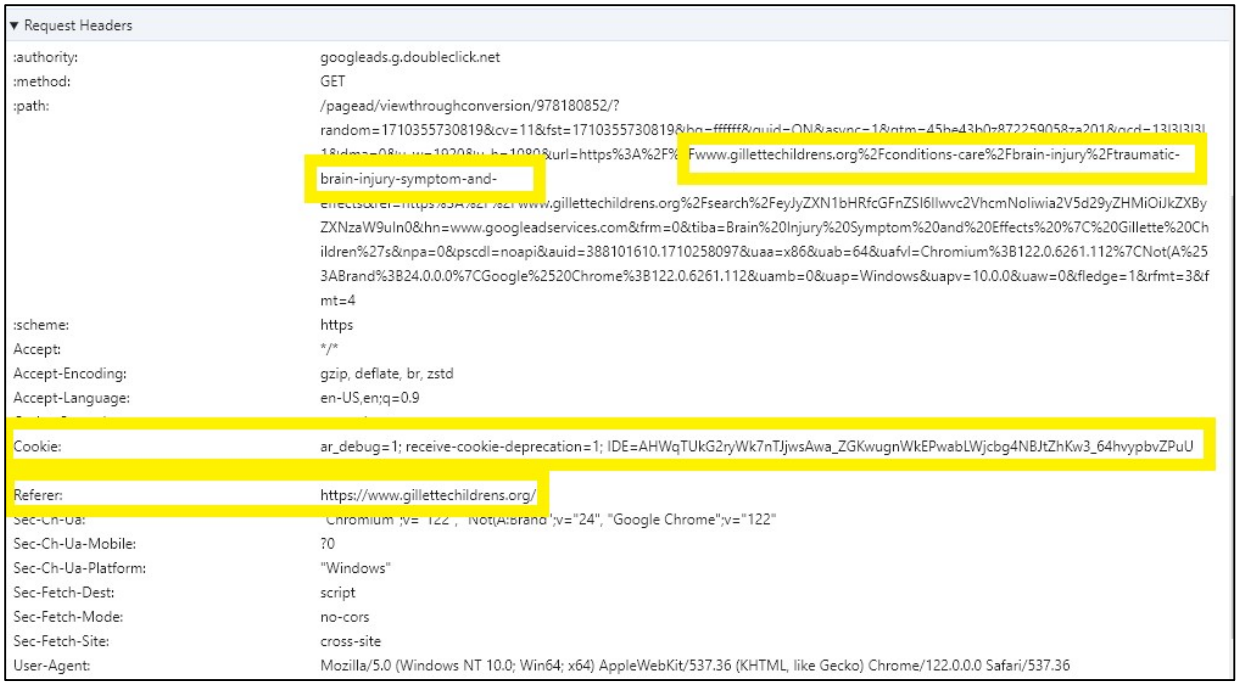

Figure 7: Depiction of "Brain Injury" Search Disclosed to Google

72. Also like the Meta Pixel, the Google tracking tools intercept a patient's act of requesting an appointment with a specific physician, as reflected in ***Figure 8*** below:

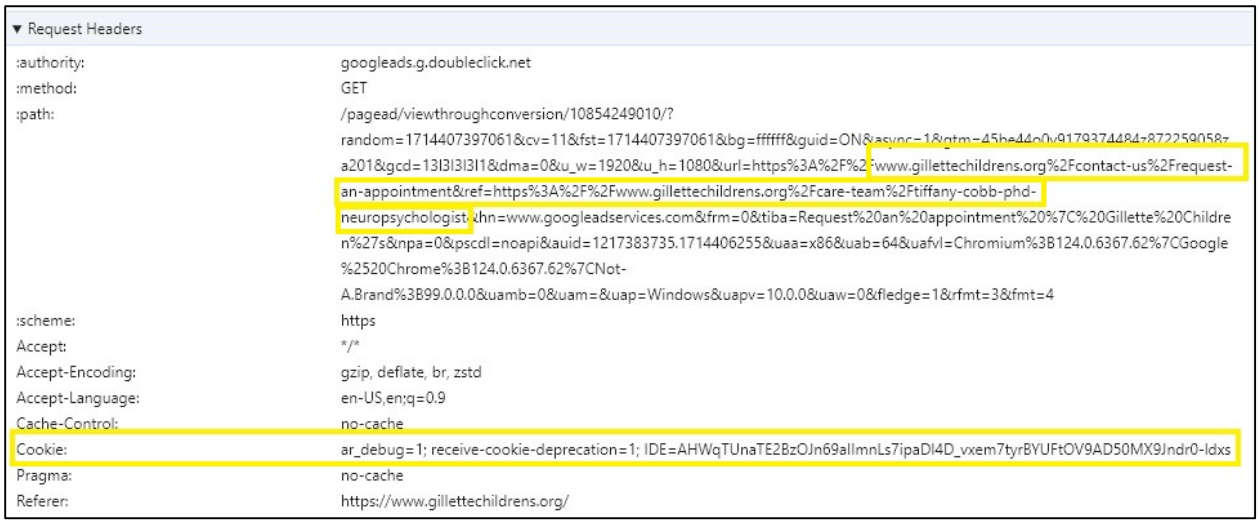

Figure 8: Depiction of Appointment Request Transmitted to Google

73. Based on the above examples of how the Tracking Tools operate on Gillette's Website, Meta and Google would know (1) that a particular individual—who Meta and

Google could identify based on their respective accounts—was a patient or prospective patient of Gillette seeking healthcare services, (2) that the named patient searched for information regarding epilepsy, seizures, brain injuries, or pediatric rehabilitation medicine, (3) that the named patient inquired about specific physicians, and (4) that the patient in question was attempting to make an appointment with specific physicians. Meta and Google would also know the named patient's location and IP address, among other identifiers associated with the patient's computer or cell phone. Using this Personal Information, the technology companies could put the named patient into a Core or Custom Audience for purposes of targeted advertising by Gillette or any other company seeking to advertise its services or products to individuals that fit the named patient's profile.

74. In this way, Gillette, Meta, Google, and other third parties profit off of Plaintiffs' and Class Members' Personal Information without their knowledge, consent, or authorization.

75. Defendant deprived Plaintiffs and the Class Members of their privacy rights when it: (a) embedded and implemented the Tracking Tools, which surreptitiously intercepted, recorded, and disclosed Plaintiffs' and other online patients' and prospective patients' confidential communications and private information; (b) disclosed patients' and prospective patients' protected information to Meta and Google—unauthorized third parties; and (c) failed to provide notice to or obtain the consent from Plaintiffs and the Class Members to share their Personal Information with others.

E. Plaintiffs' Experiences with Gillette

Plaintiff Kayla Harris

76. Plaintiff Kayla Harris visited and utilized Defendant's Website between 2022 and 2023, including multiple visits in January and February 2023.

77. As a condition of receiving Defendant's services, Plaintiff disclosed her daughter's Personal Information to Defendant on numerous occasions, and most recently in or about April 2023.

78. Plaintiff accessed Defendant's Website and Patient Portal on her cell phone and laptop to receive healthcare services from Defendant and at Defendant's direction.

79. Plaintiff has used and continues to use the same devices to maintain and access active Instagram and Google accounts throughout the relevant period in this case.

80. During the relevant time period, when the Defendant's tracking tools were present, and specifically in early 2023, Plaintiff used the Website "search" bar to search for children's [redacted]. She also used the Website to take health assessments related to her daughter's [redacted], and schedule appointments with [redacted], [redacted]. Plaintiff used both the public-facing portion of the Website and the patient portal to interact with Gillette.

81. The full scope of Defendant's interceptions and disclosures of Plaintiff's communications to Meta and Google can only be determined through formal discovery. However, Defendant intercepted at least the following communications about Plaintiff's daughter's medical condition and prospective healthcare providers. The following long-URLs or substantially similar URLs were sent to Meta and Google:

[redacted]

82. Contemporaneously with the interception and transmission of Plaintiff's communications on https://www.gillettechildrens.org regarding her daughter's [redacted], including information such as physician selected, appointments, button/menu selections and/or content typed into free text boxes, Defendant also disclosed to Meta and Google Plaintiff's personal identifiers, including but not limited to her IP address and Facebook ID.

83. Plaintiff reasonably expected that her communications with Defendant via the Website were confidential, solely between herself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

84. Plaintiff provided her daughter's Personal Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

85. As described herein, Defendant worked along with Meta and Google to intercept Plaintiff's communications, including those that contained her daughter's Personal Information.

86. Defendant willfully facilitated these interceptions without Plaintiff's knowledge, consent or express written authorization.

87. Right after or soon after submitting her daughter's Personal Information to Defendant, Plaintiff began to receive ads on her Meta accounts related to her daughter's medical condition, specifically ads for Gillette and ads related to [redacted].

88. Defendant did not inform Plaintiff that it had shared her daughter's Personal Information with Meta and Google.

89. By doing so without her consent, Defendant breached Plaintiff's and her daughter's privacy and unlawfully disclosed their Personal Information.

90. Plaintiff would not have paid (or would have paid substantially less) for Defendant's services, including her daughter's visits to Defendant's providers, tests, and treatments sought, had she known that her daughter's PHI was being disclosed to unauthorized third parties.

Plaintiff Stephanie Braulick

91. Plaintiff Stephanie Braulick visited and utilized Defendant's Website several times per week from 2019 and through the present.

92. As a condition of receiving Defendant's services, Plaintiff disclosed her son's Personal Information to Defendant on numerous occasions, and most recently in or about April 2024.

93. Plaintiff accessed Defendant's Website on her cell phone and desktop computer to receive healthcare services from Defendant and at Defendant's direction.

94. Plaintiff has used and continues to use the same devices to maintain and access active Facebook and Google accounts throughout the relevant period in this case.

95. During the relevant time period, when the Defendant's Pixels were present, and specifically from 2019 through the present, Plaintiff used the Website "search" bar to search for and type in information related to her son's medical conditions, including [redacted]. She also searched for and scheduled appointments with physicians, [redacted]. Plaintiff used both the public-facing portion of the Website and the patient portal to interact with Gillette.

96. The full scope of Defendant's interceptions and disclosures of Plaintiff's communications to Meta and Google can only be determined through formal discovery. However, Defendant intercepted at least the following communications about Plaintiff's son's prospective healthcare providers. The following long-URLs or substantially similar URLs were sent to Meta and Google:

[redacted]

[redacted]

97. Contemporaneously with the interception and transmission of Plaintiff's communications on https://www.gillettechildrens.org regarding her son's medical conditions and treatments sought, including information such as physician selected, button/menu selections and/or content typed into free text boxes, Defendant also disclosed to Meta Plaintiff's personal identifiers, including but not limited to her IP address and Facebook ID.

98. Plaintiff reasonably expected that her communications with Defendant via the Website were confidential, solely between herself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

99. Plaintiff provided her son's Personal Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

100. As described herein, Defendant worked along with Meta and Google to intercept Plaintiff's communications, including those that contained her son's Personal Information.

101. Defendant willfully facilitated these interceptions without Plaintiff's knowledge, consent or express written authorization.

102. Right after or soon after submitting her son's Personal Information to Defendant, Plaintiff began to receive ads on her Facebook account and other social media related to her son's medical conditions and Gillette's medical services. Plaintiff also received ads for Gillette while browsing the internet.

103. Defendant did not inform Plaintiff that it had shared her son's Personal Information with Meta and Google.

104. By doing so without her consent, Defendant breached Plaintiff's and her son's privacy and unlawfully disclosed their Personal Information.

105. Plaintiff would not have paid (or would have paid substantially less) for Defendant's services, including her son's visits to Defendant's providers, tests and treatments sought, had she known that her son's PHI was being disclosed to unauthorized third parties.

F. Defendant's Conduct Violates its Own Privacy Policies and Promises

106. Defendant's privacy policies represent to Plaintiffs and Class Members that Defendant will keep Personal Information private and confidential and Gillette will only disclose Personal Information under certain circumstances.

107. Defendant publishes Legal Notices that represent to patients and Website visitors that Defendant will keep sensitive information confidential and will only disclose Personal Information under certain circumstances, none of which apply here.[29]

[29] *Legal Notices*, https://www.gillettechildrens.org/legal-notices (last visited Apr. 25, 2024).

108. Defendant's Privacy Policy explains Defendant's legal duties with respect to Personal Information and the exceptions for when Defendant can lawfully use and disclose Plaintiffs' and Class Members' Personal Information:

> Gillette Children's is strongly committed to protecting the privacy of its online users: patients, families, donors, the media, and others. We do not collect personally identifiable information about individuals, except when it is knowingly provided by such individuals (e.g. web forms). We do not share voluntarily provided, personally identifiable information for any purpose other than its intended use. The only exception is described under "Donations and Fundraising Events."
>
> We do not rent or sell visitors' personal information to third parties, such as marketers.
>
> It is possible that we could be forced to disclose personally identifiable user information in response to a search warrant, subpoena, or court order; that can happen to any organization keeping records. Disclosures may also be appropriate to protect our legal rights and the security or integrity of our Web site, or to avoid liability. Those kinds of disclosures are highly unlikely, but possible.[30]

109. The Privacy Policy further represents that "cookies used by Gillette Children's do not collect any personal information about a visitor, provide any way to contact a visitor, or extract any information from a visitor's computer."[31]

110. While the Privacy Policy mentions that Defendant's web pages may contain pixels, it describes their presumably limited function as "to count users who have visited those pages or opened an e-mail and for other related Sites statistics (for example, recording the popularity of certain Sites content and verifying system and server integrity)."[32]

---

[30] *Id.*

[31] *Id.*

[32] *Id.*

111. Defendant's Privacy Policy does not permit Defendant to intercept, transmit, and/or disclose Plaintiffs' and Class Members' Personal Information to third parties, including Meta, for marketing purposes.

112. Further, while Defendant's Privacy Policy states that Defendant uses Google Analytics to provide Website users "with interest-based advertising based on [their] online activity," Google specifically advises its customers that they "must refrain from using Google Analytics in any way that may create obligations under HIPAA for Google. HIPAA-regulated entities using Google Analytics must refrain from exposing to Google any data that may be considered Protected Health Information (PHI), even if not expressly described as PII in Google's contracts and policies."[33]

113. Defendant violated its own Privacy Policy by unlawfully intercepting and disclosing Plaintiffs' and Class Members' Personal Information to Meta and other third parties without adequately disclosing that it shares Personal Information with third parties and without acquiring the specific patients' consent or authorization to share the Personal Information.

G. Exposure of Personal Information Creates a Substantial Risk of Harm

114. The FTC has recognized that consumer data is a lucrative (and valuable) form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour underscored this point by reiterating that "most consumers cannot begin to

[33] *HIPAA and Google Analytics*, https://support.google.com/analytics/answer/13297105?hl=en ("[f]or HIPAA-regulated entities looking to determine how to configure Google Analytics on their properties, the HHS Bulletin provides specific guidance on when data may and may not qualify as PHI") (last visited Apr. 25, 2024).

comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[34]

115. The FTC also issued, and regularly updates, guidelines for businesses to implement reasonable data security practices and incorporate security into all areas of the business. According to the FTC, reasonable data security protocols require, among other things: (1) using industry tested and accepted methods; (2) monitoring activity on networks to uncover unapproved activity; (3) verifying that privacy and security features function properly; and (4) testing for common vulnerabilities or unauthorized disclosures.[35]

116. The FTC cautions businesses that failure to protect Personal Information and the resulting privacy breaches can destroy consumers' finances, credit history, and reputations, and can take time, money, and patience to resolve the effect.[36] Indeed, the FTC treats the failure to implement reasonable and adequate data security measures as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

H. Plaintiffs' and the Class's Personal Information is Valuable

117. As many health care data industry experts have recognized, "[p]atients' medical data constitutes a cornerstone of the big data economy. A multi-billion dollar

[34] Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable, at 2 (Dec. 7, 2009) https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf (last visited Apr. 23, 2024).
[35] *Start With Security, A Guide for Business,* https://www.ftc.gov/business-guidance/resources/start-security-guide-business (last visited Apr. 23, 2024).
[36] *See Taking Charge: What to Do if Your Identity is Stolen*, FTC, at 2 (2012), https://www.myoccu.org/sites/default/files/pdf/taking-charge-1.pdf (last visited Apr. 23, 2024).

industry operates by collecting, merging, analyzing[,] and packaging patient data and selling it to the highest bidder."[37]

118. Thus, the personal, health, and financial information of Plaintiffs and the Class Members is valuable and has become a highly desirable commodity. Indeed, one of the world's most valuable resources is the exchange of personal data.[38]

119. Business News Daily reported that businesses collect personal data (i.e., gender, web browser cookies, IP addresses, and device IDs), engagement data (i.e., consumer interaction with a business's website, applications, and emails), behavioral data (i.e., customers' purchase histories and product usage information), and attitudinal data (i.e., consumer satisfaction data) from consumers.[39] Companies then use this data to impact the customer experiences, modify their marketing strategies, publicly disclose or sell data, and even to obtain more sensitive data that may be even more lucrative.[40]

120. The power to capture and use customer data to manipulate products, solutions, and the buying experience is invaluable to a business's success. Research shows

---

[37] Niam Yaraghi, *Who should profit from the sale of patient data?,* The Brookings Institution (Nov. 19, 2018), https://www.brookings.edu/blog/techtank/2018/11/19/who-should-profit-from-the-sale-of-patient-data/ (last visited Apr. 23, 2024).
[38] *The world's most valuable resource is no longer oil, but data* (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (last visited Apr. 23, 2024).
[39] Max Freedman, *How Businesses Are Collecting Data (And What They're Doing With It)* (Aug. 5, 2022; updated May 30, 2023), https://www.businessnewsdaily.com/10625-businesses-collecting-data.html (last visited Apr. 23, 2024).
[40] *Id.*

that organizations who "leverage customer behavioral insights outperform peers by 85 percent in sales growth and more than 25 percent in gross margin."[41]

121. In 2013, the Organization for Economic Cooperation and Development ("OECD") published a paper entitled "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value."[42] In this paper, the OECD measured prices demanded by companies concerning user data derived from "various online data warehouses."[43]

122. OECD indicated that "[a]t the time of writing, the following elements of personal data were available for various prices: USD 0.50 cents for an address, USD 2 [i.e., $2] for a date of birth, USD 8 for a social security number (government ID number), USD 3 for a driver's license number and USD 35 for a military record. A combination of address, date of birth, social security number, credit record and military is estimated to cost USD 55."[44]

123. Unlike financial information, such as credit card and bank account numbers, the PHI and certain PII cannot be easily changed. Dates of birth and social security numbers are given at birth and attach to a person for the duration of his or her life. Medical histories

---

[41] Brad Brown, et al. *Capturing value from your customer data* (Mar. 15, 2017), https://www.mckinsey.com/business-functions/quantumblack/our-insights/capturing-value-from-your-customer-data (last visited Apr. 23, 2024).
[42] Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD Digital Economy Papers, No. 220, OECD PUBLISHING PARIS (Apr. 2, 2013), https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf (last visited Apr. 23, 2024).
[43] *Id.* at 25.
[44] *Id.*

are inflexible. For these reasons, these types of information are the most lucrative and valuable.[45]

124. Consumers place considerable value on their Personal Information and the privacy of that information. One 2002 study determined that U.S. consumers highly value a website's protection against improper access to their Personal Information, between $11.33 and $16.58 per website. The study further concluded that to U.S. consumers, the collective "protection against errors, improper access, and secondary use of personal information is worth between US$30.49 and $44.62.[46] This data is approximately twenty years old, and the dollar amounts would likely be exponentially higher today.

125. Time Magazine published an article in 2017 titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry" in which it described the extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.[47]

126. Similarly, CNBC published an article in 2019 in which it observed that "[d]e-identified patient data has become its own small economy: There's a whole market of

---

[45] *Calculating the Value of a Data Breach – What Are the Most Valuable Files to a Hacker?* Donnellon McCarthy Enters (July 21, 2020), https://www.dme.us.com/2020/07/21/calculating-the-value-of-a-data-breach-what-are-the-most-valuable-files-to-a-hacker/ (last visited Apr. 23, 2024).

[46] Il-Horn Hann, Kai-Lung Hui *et al.*, *The Value of Online Information Privacy: Evidence from the USA and Singapore,* at 17, Marshall Sch. Bus., Univ. So. Cal. (Oct. 2002), https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited Apr. 23, 2024).

[47] *See* https://time.com/4588104/medical-data-industry/ (last visited Apr. 16, 2023).

brokers who compile the data from providers and other health-care organizations and sell it to buyers."[48]

127. Indeed, numerous marketing services and consultants offering advice to companies on how to build their email and mobile phone lists—including those seeking to take advantage of targeted marketing—direct putative advertisers to offer consumers something of value in exchange for their personal information. "No one is giving away their email address for free. Be prepared to offer a book, guide, webinar, course or something else valuable."[49]

128. There is also a market for data in which consumers can participate. Personal information has been recognized by courts as extremely valuable. *See In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) ("Neither should the Court ignore what common sense compels it to acknowledge—the value that personal identifying information has in our increasingly digital economy. Many companies, like Marriott, collect personal information. Consumers too recognize the value of their personal information and offer it in exchange for goods and services.").

129. Several companies have products through which they pay consumers for a license to track their data. Google, Nielsen, UpVoice, HoneyGain, and SavvyConnect are all companies that pay for browsing historical information.

---

[48] *See* https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html (last visited Apr. 21, 2024).

[49] VERO, HOW TO COLLECT EMAILS ADDRESSES ON TWITTER https://www.getvero.com/resources/twitter-lead-generation-cards/. (last visited Apr. 21, 2024).

130. Facebook also has paid users for their digital information, including browsing history. Until 2019, Facebook ran a "Facebook Research" app through which it paid $20 a month for a license to collect browsing history information and other communications from consumers between the ages 13 and 35.

131. Additionally, healthcare data is extremely valuable to bad actors. Health care records may be valued at up to $250 per record on the black market.[50]

132. Defendant's privacy violations exposed a variety of Personal Information, including patient status, health conditions and symptoms, physicians, and other highly sensitive data.

133. PHI, like that exposed here, is likely even more valuable than Social Security numbers and just as capable of being misused.[51] PHI can be ten times more valuable than credit card information.[52] This is because one's personal health history, including prior illness, surgeries, diagnoses, mental health, prescriptions, and the like cannot be changed or replaced, unlike credit card information and even, under difficult circumstances, Social Security numbers.[53]

---

[50] Tori Taylor, *Hackers, Breaches, and the Value of Healthcare Data, SecureLink* (June 30, 2021), https://www.securelink.com/blog/healthcare-data-new-prize-hackers.

[51] *FBI Cyber Division Bulletin: Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI (April 8, 2014), https://publicintelligence.net/fbi-health-care-cyber-intrusions/#:~:text=(U)%20Cyber%20actors%20will%20likely,records%20in%20the%20black%20market. (last visited Apr. 23, 2024).

[52] Tim Greene, *Anthem hack: Personal data stolen sells for 10x Price of Stolen Credit Card Numbers*, https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Apr. 23, 2024)).

134. Some industry insiders and journalists are even calling hospitals the "brokers to technology companies" for their role in data sharing in the $3 trillion healthcare sector.[54] "Rapid digitization of health records . . . have positioned hospitals as a primary arbiter of how much sensitive data is shared."[55]

I. Plaintiffs and the Class Had a Reasonable Expectation of Privacy in Their Interaction with Defendant's Website

135. Consumers assume the data they provide to hospitals will be kept secure and private.

136. In a recent survey related to Internet user expectations, most website visitors indicated that their detailed interactions with a website should only be used by the website and not be shared with a party they know nothing about.[56] Thus, website visitors reasonably expect that their interactions with a website should not be released to third parties unless explicitly stated.[57]

---

[53] *Hackers Selling Healthcare Data in the Black Market*, INFOSEC (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Apr. 23, 2024).

[54] Melanie Evans, *Hospitals Give Tech Giants Access to Detailed Medical Records* (Jan. 20, 2020), https://www.wsj.com/articles/hospitals-give-tech-giants-access-to-detailed-medical-records-11579516200 (last visited Apr. 23, 2024).

[55] *Id.*

[56] *See Privacy and Online Tracking Perceptions Survey Report* (March 2020), CUJOAI, at 15–19, Privacy Survey_03-24 (cujo.com) (indicating major concerns of survey respondents was illegal use of data and unethical tracking and indicating respondents' belief that responsibility allocation falls on websites, and Internet users should be able to turn to the websites themselves, for privacy breaches).

[57] Frances S. Grodzinsky, Keith W. Miller & Marty J. Wolf, *Session Replay Scripts: A Privacy Analysis*, THE INFORMATION SOCIETY, 38:4, 257, 258 (2022).

137. The majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares its' customers' data.[58] A March 2000 BusinessWeek/Harris Poll found that 89 percent of respondents were uncomfortable with web tracking schemes where data was combined with an individual's identity.[59] The same poll found that 63 percent of respondents were uncomfortable with web tracking even where the clickstream data was not linked to personally identifiable information.[60] A July 2000 USA Weekend Poll showed that 65 percent of respondents thought that tracking computer use was an invasion of privacy.[61]

138. Patients and website users act consistently with their expectation of privacy. For example, following a new rollout of the iPhone operating software—which asks users for clear, affirmative consent before allowing companies to track users—85 percent of worldwide users and 94 percent of U.S. users chose not to allow such tracking.[62]

139. Like the greater population, Defendant's patients and prospective patients would expect the highly sensitive medical information they provided to Defendant through the Website to be kept secure and private.

J. Defendant's Conduct Violates HIPAA

140. Under HIPAA, individuals' health information must be:

> properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health

[58] *Public Opinion on Privacy*, EPIC.ORG, https://archive.epic.org/privacy/survey/.
[59] *Id.*
[60] *Id.*
[61] *Id.*
[62] Margaret Taylor, *How Apple screwed Facebook* (May 19, 2021), https://www.wired.co.uk/article/apple-ios14-facebook.

> and well-being. The [Privacy] Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing.[63]

141. HIPAA "is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge."[64] The rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

142. HIPAA defines "protected health information" as "individually identifiable health information" that is "created or received by a health care provider" (or similar entities) that "[r]elates to past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual." 45 C.F.R. § 160.103. Identifiers such as patient-status (i.e., information that connects a particular user to a particular health care provider), medical conditions, health symptoms, treatments, and physicians, gathered in this case by the Tracking Tools through Gillette's Website, constitute protected health information.

---

[63] *Summary of the HIPAA Privacy Rule* (Oct. 19, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last visited Apr. 17, 2024).

[64] *Health Insurance Portability and Accountability Act of 1996 (HIPAA)* (June 27, 2022), https://www.cdc.gov/phlp/publications/topic/hipaa.html#:~:text=Health%20Insurance%20Portability%20and%20Accountability%20Act%20of%201996%20(HIPAA),-On%20This%20Page&text=The%20Health%20Insurance%20Portability%20and,the%20patient's%20consent%20or%20knowledge (last visited Apr. 19, 2024).

143. To ensure protection of this private and sensitive information, HIPAA mandates standards for handling PHI—the very data Defendant failed to protect. According to the U.S. Department of Health and Human Services' Health Information Privacy Bulletin ("HHS Privacy Bulletin"), HIPAA covered entities cannot share PHI or PII to online tracking technology vendors for marketing purposes without first obtaining the individual's HIPAA-compliant authorization.[65] The HHS Privacy Bulletin explicitly states:

> The HIPAA Rules apply when the information that regulated entities collect through tracking technologies or disclose to tracking technology vendors includes protected health information (PHI). Some regulated entities may share sensitive information with online tracking technology vendors and such sharing may be unauthorized disclosures of PHI with such vendors**. Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules.** For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.[66]

144. The HHS Privacy Bulletin also identifies several harms that may result from an impermissible disclosure of an individual's PHI, including:

> identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI. Such disclosures can reveal incredibly sensitive information about an individual, including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment.
>
> While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, because of the proliferation of

[65] *See Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, *supra*, note 5.
[66] *Id.* (internal citations omitted) (emphasis in original).

> tracking technologies collecting sensitive information, OCR is providing this reminder that it is critical for regulated entities to ensure that they disclose PHI **only** as expressly permitted or required by the HIPAA Privacy Rule.[67]

145. According to HHS, "[s]ome regulated entities may be disclosing a variety of information to tracking technology vendors through tracking technologies placed on the regulated entity's website or mobile app, such as information that the individual types or selects when they use regulated entities' websites or mobile apps." The "information disclosed might include an individual's medical record number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, device IDs, or any unique identifying code."[68]

146. Individually identifiable health information ("IIHI") "collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as in some circumstances IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services."[69]

147. Thus, when a regulated entity, again like Defendant, collects the individual's information, that information connects the individual to the regulated entity (i.e., it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or health care or payment for care.

---

[67] *Id.* (internal citations omitted) (emphasis in original).
[68] *Id.*
[69] *Id.*

148. Further, the HHS Privacy Bulletin makes clear that the use of tracking technologies on the public-facing or "unauthenticated" portion of a hospital's website can likewise result in the unlawful disclosure of PHI. According to the HHS Privacy Bulletin, "in some cases, tracking technologies on unauthenticated webpages may have access to PHI, in which case the HIPAA Rules apply to the regulated entities' use of tracking technologies and disclosures to the tracking technology vendors."[70] For example, "if an individual were looking at a hospital's webpage listing its oncology services to seek a second opinion on treatment options for their brain tumor, the collection and transmission of the individual's IP address, geographic location, or other identifying information showing their visit to that webpage is a disclosure of PHI to the extent that the information is both identifiable and related to the individual's health or future health care."[71]

149. When Plaintiffs communicated with Gillette regarding "treatment options" and other health-related information on the Gillette Website, the Tracking Tools intercepted and disclosed those communications to Meta and Google in violation of HIPAA's Privacy Rule.

CLASS ACTION ALLEGATIONS

150. Plaintiffs bring this class action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of themselves and all others similar situated.

151. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

> All individuals residing in the United States whose Personal Information was disclosed to a third party through Defendant's

[70] *Id.*
[71] *Id.*

> Website without authorization or consent during the applicable statute of limitations period.

152. The Minnesota Sub-Class that Plaintiffs seek to represent is defined as follows:

> All individuals residing in the State of Minnesota whose Personal Information was disclosed to a third party through Defendant's Website without authorization or consent during the applicable statute of limitations period.

153. Excluded from the Classes is Defendant; officers, directors, and employees of Defendant; any entity in which Defendant has a controlling interest in, is a parent or subsidiary of, or which is otherwise controlled by Defendant; and Defendant's affiliates, legal representatives, attorneys, heirs, predecessors, successors, and assignees. Also excluded are the Judges and Court personnel in this case and any members of their immediate families.

154. Plaintiffs reserve the right to modify and/or amend the Class definitions, as necessary.

155. All members of the proposed Classes are readily identifiable through Defendant's records.

156. All requirements for class certification under Fed. R. Civ. P. 23(a), 23(b)(2) and 23(b)(3) are satisfied.

157. **Numerosity**. The members of the Classes are so numerous that joinder of all members of the Classes is impracticable. Plaintiffs are informed and believe that the proposed Classes includes tens of thousands of people based on Gillette's reported patient

visits per year. The precise number of the Class Members is unknown to the Plaintiffs but may be ascertained from Defendant's records.

158. **Commonality and Predominance.** This action involves common questions of law and fact to the Plaintiffs and the Class Members, which predominate over any questions only affecting individual Class Members. These common legal and factual questions include, without limitation:

a. Whether Plaintiffs' and Class Members' private communications were intercepted and disclosed;

b. Whether the interception and disclosure of Plaintiffs' and Class Members' communications was consensual;

c. Whether Defendant owed Plaintiffs and the other Class Members a duty to adequately protect their Personal Information;

d. Whether Defendant owed Plaintiffs and the other Class Members a duty to secure their Personal Information from interception and disclosure via third-party tracking technologies;

e. Whether Defendant owed Plaintiffs and the other Class Members a duty to implement reasonable data privacy protection measures because Defendant accepted, stored, created, and maintained highly sensitive information concerning Plaintiffs and the Classes;

f. Whether Defendant knew or should have known of the risk of disclosure of data through third-party tracking technologies;

g. Whether Defendant breached its duty to protect the Personal Information of Plaintiffs and the other Class Members;

h. Whether Defendant knew or should have known about the inadequacies of its privacy protection;

i. Whether Defendant failed to use reasonable care and reasonable methods to safeguard and protect Plaintiffs' and the Classes' Personal Information from unauthorized disclosure;

j. Whether proper data security measures, policies, procedures, and protocols were enacted within Defendant's computer systems to safeguard and protect Plaintiffs' and the Classes' Personal Information from unauthorized disclosure;

k. Whether Defendant's conduct was the proximate cause of Plaintiffs' and the Classes' injuries;

l. Whether Plaintiffs and the Class Members had a reasonable expectation of privacy in their Personal Information;

m. Whether Plaintiffs and the Class Members suffered ascertainable and cognizable injuries as a result of Defendant's misconduct;

n. Whether Plaintiffs and the Class Members are entitled to recover damages; and

o. Whether Plaintiffs and the Class Members are entitled to other appropriate remedies including injunctive relief.

159. Defendant engaged in a common course of conduct giving rise to the claims asserted by Plaintiffs on behalf of themselves and the Classes. Individual questions, if any, are slight by comparison in both quality and quantity to the common questions that control this action.

160. **Typicality.** Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Personal Information, like that of every other Class Member, was improperly disclosed by Defendant. Defendant's misconduct impacted all Class Members in a similar manner.

161. **Adequacy.** Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class and have retained counsel experienced in complex consumer class action litigation and intend to prosecute this action vigorously. Plaintiffs have no adverse or antagonistic interests to those of the Classes.

162. **Superiority.** A class action is superior to all other available methods for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class Members are relatively small compared to the burden and expense that would be entailed by individual litigation of their claims against Defendant. The adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudications of the asserted claims. There will be no difficulty in managing this action as a class action, and the disposition of the claims of the Class Members in a single action will provide substantial benefits to all parties and to the Court. Absent a class action, individual patients like Plaintiffs would find the cost of

litigating their claims prohibitively high and would have no effective remedy for monetary relief.

163. Class Certification under Fed. R. Civ. P. 23(b)(2) is also appropriate. Defendant has acted or refused to act on grounds that apply generally to the Classes, thereby making monetary, injunctive, equitable, declaratory, or a combination of such relief appropriate. As Defendant continues to engage in the practices described herein, the risk of future harm to Plaintiffs and the Classes remains, making injunctive relief appropriate. The prosecution of separate actions by all affected individuals with injuries similar to Plaintiffs', even if possible, would create a substantial risk of (a) inconsistent or varying adjudications with respect to individual patients, which would establish potentially incompatible standards of conduct for Defendant, and/or (b) adjudications with respect to individual patients which would, as a practical matter, be dispositive of the interests of the other patients not parties to the adjudications, or which would substantially impair or impede the ability to protect the interests of the Classes. Further, the claims of individual patients in the defined Classes are not sufficiently large to warrant vigorous individual prosecution considering all of the concomitant costs and expenses.

LEGAL CLAIMS

COUNT I
Violation of the Electronic Communications Privacy Act ("ECPA")
18 U.S.C. § 2511(1)
(By Plaintiffs and on behalf of the Nationwide Class)

164. Plaintiffs reallege and incorporate by reference every allegation contained in the paragraphs above as though fully set forth herein.

165. The Electronic Communications Privacy Act ("ECPA") protects against the intentional interception, attempted interception, or the procurement of another person to intercept or attempt to intercept any wire, oral, or electronic communication. *See* 18 U.S.C. § 2511(1)(a).

166. The ECPA further provides any person who:

> (c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;
>
> (d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection.
>
> Shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

Id. §§ 2511(1)(c) & (d).

167. The primary purpose of the ECPA is to protect the privacy and security of communications as technology evolves.

168. Section 2520 provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used. Specifically, Section 2520 states that "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of [Chapter 119] may in a civil action recover from the person or entity . . ., which engaged in that violation" in a civil action. *Id.* § 2520(a).

169. Section 2520 provides for $10,000 in statutory damages for violations of ECPA. *Id.* § 2520(c)(2)(B).

170. The ECPA defines "intercept[ion]" as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." *Id.* § 2510(4).

171. The ECPA defines "contents," when used with respect to electronic communications, to "include[] any information concerning the substance, purport, or meaning of that communication." *Id.* § 2510(8).

172. "Electronic communication" means "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." *Id*. § 2510(12).

173. "Electronic, mechanical or other device" means "any device or apparatus which can be used to intercept . . . electronic communication[s]." *Id.* § 2510(5). Here, Plaintiffs' and the Class Members' browsers and computing devices and Defendant's webservers, Website, and Pixel code and other tracking technologies Defendant deployed are all "devices" for the purposes of the ECPA.

174. The transmissions of PII and PHI from Plaintiffs and the Class Members to Defendant through Defendant's Website are "electronic communications" under the ECPA. *See id*. § 2510(12). The information transmitted by Plaintiffs and the Class Members included, but was not limited to, information regarding patient status, past and

current health conditions and symptoms, treatments and care options, physicians, location, and other sensitive information.

175. Additionally, through its use of the Tracking Tools, Defendant intercepted and disclosed the communications about patient status, health conditions and symptoms, and other Personal Information Plaintiffs searched for on Defendant's Website. This information was, in turn, used by third-parties, such as Meta and Google, to 1) place Plaintiffs in specific health-related categories; and 2) target Plaintiffs with particular advertising associated with their particular health conditions. Defendant knowingly transmitted this data and did so for the purpose of financial gain.

176. By embedding and deploying the Tracking Tools on Defendant's Website, Defendant intentionally violated the ECPA, through its interception, attempt at interception, and its procurement of third parties to intercept the electronic communications of Plaintiffs and the Class Members. Defendant also intentionally used or attempted to use the contents of Plaintiffs' and the Class Members' electronic communications, knowing that the information was obtained through interception. Defendant's use of the intercepted information and data for its own advertising and data analytics, in the absence of express written consent, violated ECPA.

177. Further, by embedding the Tracking Tools on its Website and disclosing the content of patient communications relating to Personal Information, without consent, Defendant had a purpose that was tortious, criminal, and designed to violate state and federal laws, including:

a. An invasion of privacy;

b. A violation of the Minnesota Uniform Deceptive Trade Practices Act, Mn. Stat. §325D.43-48;

c. A violation of 42 U.S.C. § 1320d–6, the Administrative Simplification subtitle of HIPAA, which protects against the disclosure of individually identifiable health information to another person and is a criminal offense punishable by fine or imprisonment; and

d. A violation of HIPAA.

178. Any party exception in 18 U.S.C. § 2511(2)(d) does not apply. The party exception in § 2511(2)(d) does not permit a party that intercepts or causes interception to escape liability if the communication is intercepted for the purpose of committing any tortious or criminal act in violation of the Constitution or laws of the United States or of any State. Here, as alleged above, Defendant violated a provision of the Health Insurance Portability and Accountability Act, specifically 42 U.S.C. § 1320d-6(a)(3).

179. 42 U.S.C. § 1320d-6(a)(3) provides criminal and civil penalties against a healthcare provider who "knowingly . . . discloses individually identifiable health information to another person." Section 1320d(6) of HIPAA defines individually identifiable health information ("IIHI") as:

> any information, including demographic information collected from an individual, that—(A) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (B) *relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual,* or the past, present, or future payment for the provision of health care to an individual, and—(i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

42 U.S.C. § 1320d(6) (emphasis added).

180. Guidance issued by HHS confirms that the Tracking Tools deployed by Defendant violate HIPAA. HIPAA prohibits disclosing patients' health information via tracking technologies on both user-authenticated webpages (such as the log-in portal) and unauthenticated webpages. The guidance includes in the definition of IIHI the types of information intercepted by the Tracking Tools on Defendant's Website, including information that "relates to the past, present, or future physical or mental health or condition of an individual," such as information about a person's symptoms, conditions, treatments, and physicians. Defendant's use of the Tracking Tools violates HIPAA because the Meta Pixel and the other Tracking Tools also transmit information that "identifies the individual" or, at a minimum, "there is a reasonable basis to believe that the information can be used to identify the individual," such as through unique identifying cookies and users' IP addresses. As described above, Plaintiffs entered data on Defendant's Website relating to health conditions and other Personal Information, and later received related advertisements from Gillette. This shows that through the Tracking Tools employed, Defendant disclosed the individually identifiable health information of its Website visitors to third parties in violation of the ECPA.

181. At no time did Plaintiffs and the Class Members provide their consent to Defendant's disclosure of their Personal Information to Meta, Google, and/or other third parties. Plaintiffs and the Class had a reasonable expectation that Defendant would not re-direct their communications content to Meta, Google, or others attached to their personal identifiers in the absence of their knowledge or consent.

182. Further, Defendant has improperly profited from its invasion of Plaintiffs' and the Class Members' privacy in its use of their data for its economic value.

183. Defendant knew that such conduct would be highly offensive. Regardless, it proceeded to embed the Tracking Tools and use them to the detriment of visitors to its Website.

184. Plaintiffs and the Class Members are entitled to damages, including statutory, compensatory and/or nominal damages in an amount to be proven at trial.

185. Defendant's conduct is ongoing, and it continues to unlawfully disclose and use the intercepted communications of Plaintiffs and the Class Members any time they provide information to Defendant through its Website without their consent. Plaintiffs and the Class Members are therefore entitled to declaratory and injunctive relief. Such relief will prevent future unlawful and unauthorized disclosure of Plaintiffs' and the Class Members' Personal Information.

COUNT II
Invasion of Privacy
(By Plaintiffs and on behalf of the Nationwide Class)

186. Plaintiffs reallege and incorporate by reference every allegation contained in the paragraphs above as though fully set forth herein.

187. The Personal Information of Plaintiffs and Class Members consists of private and confidential facts and information that were never intended to be shared beyond private communications.

188. Plaintiffs and Class Members had a legitimate expectation of privacy regarding their Personal Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

189. Defendant owed a duty to Plaintiffs and Class Members to keep their Personal Information confidential.

190. Defendant's unauthorized disclosure of Plaintiffs' and Class Members' Personal Information to Meta and Google, two of the largest advertising companies in the world, is highly offensive to a reasonable person.

191. Defendant's willful and intentional disclosure of Plaintiffs' and Class Members' Personal Information constitutes an intentional interference with Plaintiffs' and Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

192. Defendant's conduct constitutes an intentional physical or sensory intrusion on Plaintiffs' and Class Members' privacy because Defendant facilitated Meta and Google's simultaneous collection and exploitation of confidential communications.

193. Defendant failed to protect Plaintiffs' and Class Members' Personal Information and acted knowingly when it installed the Tracking Tools onto its Website because the purpose of the Tracking Tools is to track and disseminate individual's communications with the Website for the purpose of marketing and advertising.

194. Because Defendant intentionally and willfully incorporated the Tracking Tools into its Website and encouraged patients to use that Website for healthcare purposes,

Defendant had notice and knew that its practices would cause injury to Plaintiffs and Class Members.

195. As a proximate result of Defendant's acts and omissions, the private and sensitive Personal Information of Plaintiffs and Class Members was disclosed to third parties without authorization, causing Plaintiffs and the Class to suffer damages.

196. Plaintiffs, on behalf of themselves and Class Members, seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, loss of time and opportunity costs, plus prejudgment interest, and costs.

197. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their Personal Information is still maintained by Defendant and still in the possession of Meta and Google and the wrongful disclosure of the information cannot be undone.

198. Plaintiffs and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not undo Defendant's disclosure of the information to Meta and Google, who on information and belief, continue to possess and utilize that information.

199. Plaintiffs, on behalf of themselves and Class Members, further seek injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiffs' and Class Members' Personal Information and to adhere to its common law, contractual, statutory, and regulatory duties.

COUNT III
Negligence
(By Plaintiffs and on behalf of the Nationwide Class)

200. Plaintiffs reallege and incorporate by reference every allegation contained in the paragraphs above as though fully stated herein.

201. Medical providers have a duty to their patient to keep their patients' Personal Information completely confidential. *See* Minn. Stat. § 144.651 subd. 15-16; Minn. Stat. § 144.293.

202. Plaintiffs and Class Members had reasonable expectations of privacy in their communications exchanged with Defendant, including communications exchanged on Defendant's Website.

203. Contrary to its duties as a medical provider, Defendant negligently installed the Tracking Tools to disclose and transmit to third parties Plaintiffs' and Class Members' communications with Defendant, including Personal Information and the contents of such information.

204. These disclosures were made without Plaintiffs' or Class Members' knowledge, consent, or authorization, and were unprivileged.

205. The third-party recipients included, but may not be limited to, Meta and Google.

206. As a direct and proximate cause of Defendant's unauthorized disclosures of patient personally identifiable, non-public medical information, and communications, Plaintiffs and Class Members were damaged by Defendant's breach in that:

a. Personal Information that Plaintiffs and Class Members intended to remain private is no longer private;

b. Plaintiffs and Class Members face ongoing harassment and embarrassment in the form of unwanted targeted advertisements;

c. Defendant eroded the essential confidential nature of the provider-patient relationship;

d. Plaintiffs and Class Members have suffered general and compensatory damages that were proximately caused by Defendant's negligence, in an amount to be determined by a jury;

e. Defendant took something of value from Plaintiffs and Class Members and derived benefit therefrom without Plaintiffs' and Class Members' knowledge or informed consent and without compensation for such data;

f. Plaintiffs and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality;

g. Defendant's negligent actions diminished the value of Plaintiffs' and Class Members' Personal Information; and

h. Defendant's breach of its duties as a medical provider was the proximate cause of Plaintiffs' and Class Members' injuries. But for Defendant's decision to install the invisible Tracking Tools on its Website, Plaintiffs' and Class Members' Personal Information would not have been shared without their consent with Meta and other unauthorized third parties.

COUNT IV
Breach of Implied Contract
(By Plaintiffs and on behalf of the Nationwide Class)

207. Plaintiffs reallege and incorporate by reference every allegation contained in the paragraphs above as though fully stated herein.

208. As a condition of utilizing Defendant's Website and receiving services from Defendant's healthcare facilities and professionals, Plaintiffs and Class Members provided their Personal Information and compensation for their medical care.

209. When Plaintiffs and Class Members provided their Personal Information to Defendant, they entered into an implied contract pursuant to which Defendant agreed to safeguard and not disclose their Personal Information without consent.

210. Plaintiffs and Class Members would not have entrusted Defendant with their Personal Information in the absence of an implied contract between them and Defendant obligating Defendant to not disclose Personal Information without consent.

211. Plaintiffs and Class Members would not have retained Defendant to provide healthcare services in the absence of an implied contract between them and Defendant obligating Defendant not to disclose Personal Information without consent.

212. Defendant breached these implied contracts by disclosing Plaintiffs' and Class Members' Personal Information without consent to third parties like Meta and Google.

213. As a direct and proximate result of Defendant's breaches of these implied contracts, Plaintiffs and Class Members sustained damages as alleged in this Complaint,

including, but not limited to, the loss of the benefit of their bargain and diminution in value of Personal Information.

214. Plaintiffs and Class Members are entitled to compensatory and consequential damages as a result of Defendant's breach of implied contract.

COUNT V
Unjust Enrichment
(By Plaintiffs and on behalf of the Nationwide Class)

215. Plaintiffs reallege and incorporate by reference every allegation contained in the paragraphs above as though fully stated herein.

216. Defendant benefits from the use of Plaintiffs' and Class Members' Personal Information and unjustly retained those benefits at their expense.

217. Plaintiffs and Class Members conferred a benefit upon Defendant in the form of Personal Information that Defendant collected from Plaintiffs and Class Members, without authorization and proper compensation. Defendant consciously collected and used this information for its own gain, providing Defendant with economic, intangible, and other benefits, including substantial monetary compensation.

218. Defendant unjustly retained those benefits at the expense of Plaintiffs and Class Members because Defendant's conduct damaged Plaintiffs and Class Members, all without providing any commensurate compensation to Plaintiffs and Class Members.

219. The benefits that Defendant derived from Plaintiffs and Class Members was not offered by Plaintiffs and Class Members gratuitously and rightly belongs to Plaintiffs and Class Members. It would be inequitable under unjust enrichment principles in Minnesota and every other state for Defendant to be permitted to retain any of the profit or

other benefits wrongly derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

220. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class Members all unlawful or inequitable proceeds that Defendant received, and such other relief as the Court may deem just and proper.

COUNT VI
Minnesota Uniform Deceptive Trade Practices Act ("MUDTPA"), Mn. Stat. §325D.43-48
(By Plaintiffs and on behalf of the Minnesota Class)

221. Plaintiffs reallege and incorporate by reference every allegation contained in the paragraphs above as though fully stated herein.

222. The MUDTPA prohibits deceptive trade practices in a person's business, vocation, or occupation. *See* Minn. Stat. §325D.44, subd. 1.

223. Defendant is subject to the rules and statutory requirements of Minn. Stat. §325D.44 because it advertised, offered, or sold goods or services in Minnesota and therefore engaged in business directly or indirectly affecting the people of Minnesota.

224. Defendant violated Minn. Stat. §325D.44, including, but not limited to, the provisions where the person:

> represents that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have or that a person has a sponsorship, approval, status, affiliation, or connection that the person does not have; Minn. Stat. §325D.44, subd.1(5).
>
> represents that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another; and
>
> engages in any other conduct which similarly creates a likelihood of confusion or of misunderstanding. Minn. Stat. §325D.44, subd.1(7).

225. Defendant engaged in unfair, abusive, and deceptive acts, omissions, and practices in connection with consumer transactions, in violation of Sections Minn. Stat. § 325D.44, subd. 1(5) & (7).

226. Defendant's representations and omissions include both implicit and explicit representations through:

a. Failing to implement and maintain reasonable privacy measures to protect Plaintiffs' and the Minnesota Class's Personal Information, which was a direct and proximate cause of the Privacy violations described herein;

b. Failing to identify and remediate foreseeable privacy risks and adequately maintain privacy measures despite knowing the risk of disclosure of patients' Personal Information, which was a direct and proximate cause of the Privacy violations;

c. Failing to comply with common law and statutory duties pertaining to the privacy of Plaintiffs' and the Minnesota Class's Personal Information, including duties imposed by the HIPAA, 45 C.F.R. § 160.102 and the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Privacy violations;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and the Minnesota Class's Personal Information, including by implementing and maintaining reasonable privacy protection measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the privacy of Plaintiffs' and the Minnesota Class's Personal Information, including duties imposed by the HIPAA, 45 C.F.R. § 160.10;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately protect Plaintiffs' and the Minnesota Class's Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and the Minnesota Class's Personal Information,

including duties imposed by HIPAA, 45 C.F.R. § 160.102 or the FTC Act, 15 U.S.C. § 45.

227. Defendant's acts and practices were deceptive and unfair because Defendant knew its Website contained the Pixel and Google tracking tools and also knew that the Pixel and Google tracking tools would be unknown and/or not easily discoverable by Plaintiffs and Class Members, and that Defendant's actions caused or were likely to cause substantial injury to patients which was not reasonably avoidable by patients themselves and not outweighed by countervailing benefits to patients or to competition.

228. The injury to patients from Defendant's conduct was and is substantial because it was non-trivial, non-speculative, involved a monetary injury, and involved an unwarranted risk to the safety of their Personal Information.

229. Plaintiffs and the Minnesota Class could not have reasonably avoided injury because Defendant's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of patient healthcare decision-making and information gathering. By withholding important information from patients about the inadequacy of its privacy protections and Defendant's intentional use of Pixel and Google tracking tools on its Website, Defendant created an asymmetry of information between it and patients that precluded patients from taking action to avoid or mitigate injury.

230. Defendant also engaged in "deceptive" acts and practices in violation of Minn. Stat. § 325D.44, including:

a. Misrepresenting that the subject of a consumer transaction has performance, characteristics, or benefits it does not have which the supplier knows or should reasonably know it does not have; and

b. Misrepresenting that the subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if it is not and if the supplier knows or should reasonably know that it is not.

231. Had Defendant disclosed to Plaintiffs and the Minnesota Class that it used the Tracking Tools, which publicly disclosed sensitive, medical information, Defendant would have been unable to continue this type of business practice and it would have been forced to adopt reasonable data privacy measures and comply with the law. Defendant was trusted with sensitive and valuable PII and PHI regarding tens of thousands of patients, including Plaintiffs and the Minnesota Class. Defendant accepted the responsibility of protecting the data while keeping the state of the tracking technologies used on its site and application secret from the public.

232. Accordingly, Plaintiffs and the Minnesota Class acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

233. Defendant had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extensivity of the PII and PHI in its possession, and the generally accepted professional standards. This duty arose due to the representations and relationship between Defendant and Plaintiffs and the Minnesota Class as described herein. Defendant had exclusive or superior knowledge of the practices engaged in where private information related to health and safety was shared with third parties which Plaintiffs and the members of the Minnesota Class had no reasonable manner of obtaining in advance, giving rise to a further duty to disclose.

234. As a result of Defendant's wrongful conduct, Plaintiffs and the Minnesota Class were injured in that they never would have provided their PII and PHI to Defendant, or purchased Defendant's services, had they known or been told that Defendant failed to maintain sufficient security to keep their PII and PHI from being hacked and taken and misused by others.

235. As a direct and proximate result of Defendant's violations of the MUDTPA, Plaintiffs and the Minnesota Class have suffered harm, including financial losses related to the payments or services made to Defendant that Plaintiffs and the Minnesota Class would not have made had they known of Defendant's inadequate data security; lost control over the value of their PII and PHI; and other harm resulting from the unauthorized use of their PII and PHI, entitling them to damages in an amount to be proven at trial.

236. Plaintiffs and the Minnesota Class are at risk of future damage and harm from Defendant's deceptive and unfair practices because they are or may become patients of Defendant in the future and may have little choice but to continue to use Defendant's Website to receive proper and complete medical care.

237. Plaintiffs and the Minnesota Class seek all relief allowed by law, including reasonable attorneys' fees and costs and injunctive relief.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs respectfully pray for judgment in their favor as follows:

a. Certification of the Classes pursuant to the provisions of Fed. R. Civ. P. 23 and an order that notice be provided to all Class Members;

b. Designation of Plaintiffs as representatives of the Classes and the undersigned counsel as Class Counsel;

c. An award of damages in an amount to be determined at trial or by this Court;

d. Declaring that Defendant's past conduct was unlawful, as alleged herein;

e. Declaring Defendant's ongoing conduct is unlawful, as alleged herein;

f. Enjoining Defendant from continuing the unlawful practices described herein, and awarding such injunctive and other equitable relief as the Court deems just and proper;

g. Awarding Plaintiffs and the Class Members statutory, actual, compensatory, consequential, and nominal damages, as well as restitution and/or disgorgement of profits unlawfully obtained;

h. Awarding Plaintiffs and the Class Members pre-judgment and post-judgment interest;

i. Awarding Plaintiffs and the Class Members reasonable attorneys' fees, costs, and expenses; and

j. Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and the Classes, demand a trial by jury of any and all issues in this action so triable of right.

Respectfully submitted,

Dated: May 9, 2024

/s/ Hart L. Robinovitch

Hart L. Robinovitch (MN Bar No. 0240515)
Ryan J. Ellersick (*pro hac vice* forthcoming)
ZIMMERMAN REED LLP
14648 North Scottsdale Road, Suite 130
Scottsdale, AZ 85254
Telephone: (480) 348-6400
hart.robinovitch@zimmreed.com
ryan.ellersick@zimmreed.com

David S. Almeida (*pro hac vice* forthcoming)
Elena A. Belov (*pro hac vice* forthcoming)
ALMEIDA LAW GROUP LLC
849 W. Webster Avenue
Chicago, Illinois 60614
Telephone: (312) 576-3024
david@almeidalawgroup.com
elena@almeidalawgroup.com

Attorneys for Plaintiffs and the Putative Class